Akamai 客户案例

美国某学区成功抵御内部威胁

德克萨斯州某大型学区通过部署 Akamai 的微分段技术，成功保护东西向流量

保护应用程序安全

阻止内部攻击

提供流量视图

卓越教育的典范

2022 年，德克萨斯州一个拥有超过 75,000 名学生的大型公立学区被该州教育局评定为“A”级学区。作为卓越教育领域的典范，该学区提供优质的学习体验，鼓励每个学生追求卓越和充实的生活，激发他们实现理想。为此，该学区的技术运营部门倾力构建并维护卓越的基础架构，确保以安全的方式满足所有利益相关方对当前和未来数字内容及工具的需求。当该部门的新任网络安全负责人意识到学区安全方法的弱点时，Akamai Guardicore Segmentation 成功弥补了这一不足。

亟需消除内部威胁

该德克萨斯州学区一直依靠防火墙和地理围栏来保护其 IT 环境免受外部威胁。然而，该学区缺乏防御内部威胁的方法——特别是那些具有恶意企图的内部威胁。“如果他们能够访问一个系统，那么他们就可以轻松访问其他所有系统，”该学区的系统工程经理解释道。

Texas School District

位置

美国德克萨斯州

行业

公共部门

解决方案

Akamai Guardicore Segmentation

Akamai

由于无法监测内部系统之间的合法通信，该学区无法阻止非法的恶意东西向流量。面对这种威胁，技术运营部门（包括网络工程、系统工程和网络安全团队）认识到要利用一款全面的解决方案来降低风险。“如果我们不实施解决方案来全面保护学生和教职员工的信息安全，这将是我们的失职。”该经理继续说道。

以分阶段方式轻松实现微分段

在评估了各种方案后，该学区最终选择了 Akamai Guardicore Segmentation。“这是一款出类拔萃的解决方案。”该经理说道。

技术运营部门对其环境进行了审计，以确定哪些应用程序和系统需要通过 Akamai Guardicore Segmentation 进行保护。“我们是从一级应用程序开始，不过，我们最终要利用该解决方案保护所有应用程序。”该经理继续说道。

在 Akamai 的指导下，该学区通过精确的分段策略，快速、轻松地为高优先级应用程序（包括 Active Directory 和 SQL Server）创建了安全围栏，以消除系统之间不必要的数据流。审计和部署过程促进了跨职能协作。“我们通过团队合作，共同确定了如何标记设备和构建安全围栏等细节，是 Akamai Guardicore Segmentation 为我们奠定了合作的基础。”

安全围栏投入使用后，只要出现潜在问题，该学区就能收到警报。“除非我们允许，否则任何流量都无法通过。”该学区系统工程经理解释道。因此，该学区确信 Akamai 的解决方案可以立即保护这些应用程序。

“通过掌握某个应用程序的流量传输情况，我们可在需要时切换到拦截模式。Akamai Guardicore Segmentation 提供了一种直观便捷的方法，让我们可以分阶段地保护我们的环境，”该经理说道。

> Akamai Guardicore Segmentation 为我们提供了可准确了解环境情况的重要视图，并帮助确保我们的关键系统免受未经授权的东西向流量的威胁。
>
> —— 德克萨斯州学区系统工程经理

> “我们非常喜欢使用 Akamai Guardicore Segmentation。它易于配置和管理，对于任何想要保护自己免受内部威胁的学区而言，都是一款重要的解决方案。”
>
> ——德克萨斯州学区系统工程经理

获得增强的环境监测能力

尽管有些应用程序不适合创建安全围栏，不过，该学区现在能够监测这些应用程序与其他应用程序（如 Active Directory）之间的通信，获得有用的信息。技术运营部门的所有团队都可以看到所有创建了安全围栏的应用程序的数据流，从而基本上获得了对环境中所有系统运行情况的监测能力。“Akamai Guardicore Segmentation 提供了一个实时的视图，帮助我们了解系统运行情况，并提供了一种简单的方式来识别不必要的流量。此外，我们还可以轻松配置该解决方案，根据需要允许或阻止流量。”该经理说道。

这种监测能力使网络工程、系统工程和网络安全团队能够在需要时紧密合作，顺利解决出现的问题。“当我们收到可疑流量的告警时，Akamai 解决方案会为我们提供所需的背景信息，帮助我们制定解决方案，防止出现不需要的内容，同时确保我们的环境按需运行。”该经理解释道。

有效防止未经授权的远程访问

根据该学区系统工程经理的说法，Akamai Guardicore Segmentation 在持续帮助他们阻止网络攻击：“我们的系统经常遭受恶意 IP 地址攻击。Akamai 的解决方案可以监测异常活动（例如，Web 服务器上的异常端口活动），使我们能够有效阻止访问和潜在的攻击。”

此外，通过与其他安全工具的无缝协作，Akamai Guardicore Segmentation 进一步提升了该学区的安全态势。例如，学区使用特权访问管理 (PAM) 解决方案，为外部供应商提供对特定系统的所需访问权限。该学区并非是允许通过远程桌面协议 (RDP) 访问这些服务器，而是要求其工程部门使用 PAM 解决方案来远程管理服务器。Akamai Guardicore Segmentation 帮助防止 RDP 访问。

正如该学区系统工程经理所说，这种组合的安全措施可以防止人们像过去一样通过远程桌面访问服务器：“通过使用 Akamai 解决方案来阻止 RDP 访问，我们可以确保任何人都无法远程连接到我们的服务器环境。”

部署应用程序更自信

迄今为止，该学区已在其 500 台现有服务器中的 375 台上实施了 Akamai Guardicore Segmentation，并计划通过微分段解决方案保护所有可能存在的应用程序。“我们在不断推出新的应用程序（有时每周推出一款），这些应用程序在上线时就会利用 Akamai 解决方案提供安全保护。这让我们在部署新应用程序时更有信心，因为我们可以利用 Akamai Guardicore Segmentation 监测应用程序的工作和通信情况。”该学区的系统工程经理总结道。

扫码关注 - 获取最新云计算、云安全与 CDN 前沿资讯